384767

2006-23686-1

Rick Lederer
Assistant Vice President
Network Control Systems

2006 JAN 18 PM 3:23

OFFICE OF THE CHIEF COUNSEL

BNSF Railway Company
P.O. Box 961034
Fort Worth, TX 76161-0034

2600 Lou Menk Drive
Fort Worth, TX 76131
817-352-1300 Office
817-352-7260 Fax
Rick.Lederer@bnsf.com Email

Ms. Jo Strang
Associate Administrator for Safety

Mr. Grady Cothen
Deputy Associate Administrator for
Safety Standards and Program Development

Federal Railroad Administration
1120 Vermont Ave NW
Washington, DC 20590

Dear Ms. Strang and Mr. Cothen:

The BNSF Railway has updated their Railroad Safety Program Plan (RSPP) to serve as its principal safety document. Please find attached the latest copy of the RSPP version 1.6. This reflects the changes from version 1.5 that was completed and sent in response to the comments received from the FRA. This RSPP version 1.6 also reflects additional changes made as a result of our legal department reviews of the Hazard Severity definitions. The changes made between version 1.5 and 1.6 are listed in another attached document that outline these specifically. We look forward to your review and approval of this latest version of the RSPP.

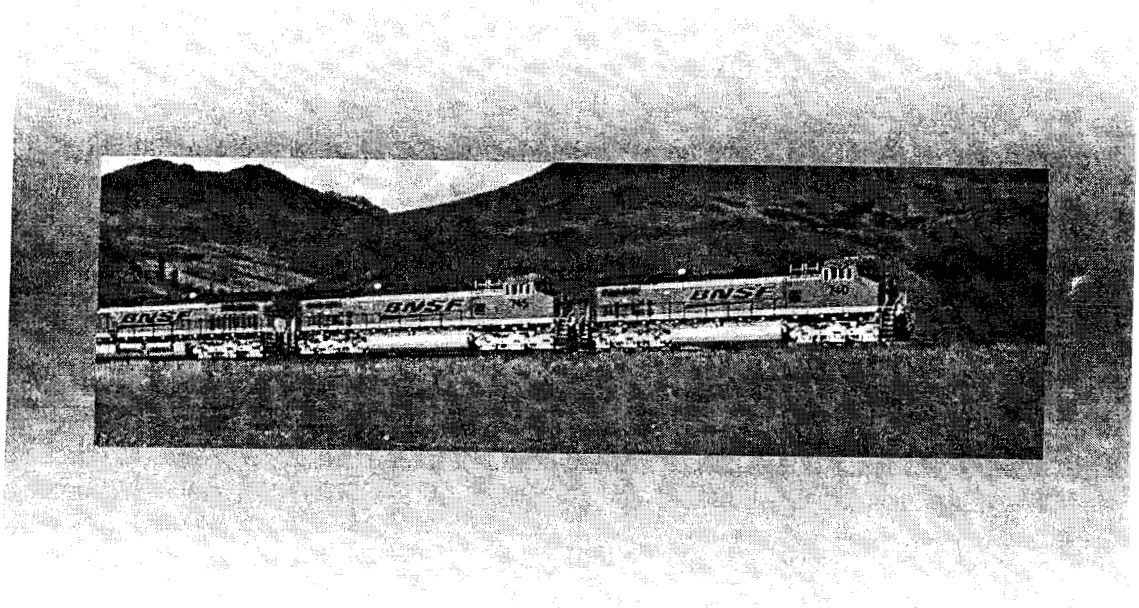
The primary contact for the Railroad Safety Program Plan as directed per 49 CFR § 236.905 will be the following:

Michael Bratcher
Senior Director, Train Control Systems
Network Control Systems BNSF Railway
2600 Lou Menk Drive
Fort Worth, TX. 76131
817-352-1332 (office)
817-352-7260 (fax)
michael.bratcher@bnsf.com (email)

Sincerely,

Rick D. Lederer
AVP Network Control Systems
BNSF Railway

BNSF℠ RAILWAY



Railroad Safety Program Plan (RSPP)

Submitted in fulfillment of 49 CFR 236, Subpart H, §236.905

REVISION	DATE	DESCRIPTION	INCORPORATED
Initial Release 1.0	07-31-03	Initial release for review of this document.	Charles Tilley
1.1	08-04-03	Corrections and additions inserted based on review.	Charles Tilley
1.2	09-02-03	Corrections made based on review.	Charles Tilley
1.3	08-29-05	Updates for Phase II and comments from the FRA Office of Safety	Charles Tilley
1.4	09-20-05	Revisions from ETMS team	Michael Bratcher
1.5	10-31-05	Revisions from FRA comments	Michael Bratcher
1.6	12-12-05	Revisions To Hazard Severity Definitions	Michael Bratcher

Table of Contents

1 Introduction

This Railroad Safety Program Plan (RSPP) is a BNSF Railway (BNSF) strategic safety planning document for the development and implementation of Safety-Critical Processor-Based Signal and Train Control Systems.

This RSPP is focused on the requirements of 49 CFR Part 236 Subpart H, "Standards for Development and Use of Processor-Based Signal and Train Control Systems; Final Rule" dated March 7, 2005. Sections 1-3 provide an introduction and overview of the RSPP and a list of the applicable systems on the BNSF. Section 4 of this RSPP provides BNSF requirements related to safety requirements and concepts, verification and validation (V&V), human factors, and configuration management, employed by the BNSF to meet the safety goals for Safety-Critical Processor-Based Signal and Train Control Systems. Sections 5 through 11 of the RSPP establish definitive requirements for a Product Safety Plan (PSP) that will be prepared for implementation, operation, and maintenance of a safety-critical processor-based signal and train control system on BNSF.

This PSP is specific to a particular system design and implementation, and represents the BNSF Railway's plans to ensure safety during the implementation of a safety-critical processor-based signal and train control system. The PSP is viewed as a living document that includes all aspects of product safety from design through implementation. A PSP must be prepared for each type of safety-critical processor based signal and train control system (or safety critical subsystem or component) deployed by the BNSF. The Product Supplier shall prepare, with the assistance of BNSF, a Product Safety Plan (PSP) that is compliant with this RSPP and with applicable FRA regulations. BNSF will supply the required supporting data to assist in the authentication of the PSP. The PSP will become a BNSF document that

demonstrates the safety capabilities of the safety-critical processor-based signal and train control system. All documentary evidence supporting the safety-critical processor-based signal and train control system PSP shall be made available for review and audit to the Federal Railroad Administration (FRA) by the BNSF and/or its designee.

Section 8 identifies the BNSF requirements for notifying the FRA of its preparation of a PSP to ensure compliance with the procedures established in this RSPP.

1.1 Scope and Purpose

This document describes the plan that will be used to ensure that any new processor based signal and train control system is specified, designed, built, verified and validated, and implemented with the proper emphasis on safety.

The purpose of this document is to provide a uniform framework for developing and implementing a system safety program of sufficient comprehensiveness to identify the hazards of the processor based signal and train control system and to impose design requirements and management controls to prevent mishaps. The function of this document is twofold: 1) to ensure that the deployment of the safety-critical processor based signal and train control system developed and implemented does not exceeds the level of safety risk that exists today; 2) to eliminate hazards or reduce the associated risk of hazards to an acceptable level.

1.2 Applicability

This RSPP applies to safety-critical processor based signal and train control systems, or safety critical subsystems, or safety critical components thereof, developed and implemented subject to the provisions of 49 CFR, Part 236, Subpart H "Standards for Development and Use of Processor-Based Signal and Train Control Systems; Final Rule." This RSPP also applies to some highway-rail crossing active warning systems that are covered under the new rule as applicable in 236 Subpart H and described in §234.275 (a). Section 3 identifies the currently known applicable systems on the BNSF. All existing processor based signal and train control systems are excluded unless specifically included in Section 3.

1.3 Document Overview

This document includes BNSF functional requirements, performance requirements, design guidelines, human factors, safety assurance processes and V&V requirements for the safe operation, configuration management, and maintenance of new processor based signal and train control systems. The document sections are listed below:

- Section 1 describes the scope of the document.
- Section 2 lists the references for this document.
- Section 3 provides a list of systems on BNSF subject to the provisions of 49 CFR Part 236 Subpart H and this RSPP.
- Section 4 presents the minimum general safety requirements for the development of processor based signal and train control systems as defined in 49 CFR Subpart H §236.905.
- Section 5 presents requirements for the development of a PSP as defined in 49 CFR Subpart H §236.907.
- Section 6 defines the minimum performance standard for processor based signal and train control systems as defined in 49 CFR Subpart H §236.909.
- Section 7 contains requirements for the implementation and operation of processor based signal and train control systems as defined in 49 CFR Subpart H §236.913.
- Section 8 delineates the review and approval process for the PSP as defined in 49 CFR Subpart H §236.905 and §236.911.
- Section 9 defines requirements for system operation and maintenance manuals as defined in 49 CFR Subpart H §236.919.
- Section 10 defines training and qualification program requirements as delineated in 49 CFR Subpart H §236.921, §236.923, §236.925, §236.927, and §236.929.
- Section 11 defines human-machine interface requirements as delineated in §236 Appendix E.

1.4 Acronyms and Definitions

The acronyms used in this document are defined as follows:

Acronym	Meaning
BNSF	BNSF Railway Company
CM	Configuration Management
CMP	Configuration Management Process
DoD	Department of Defense
CTC	Centralized Traffic Control
ETMS	Electronic Train Management System
FFT	Functional Fault Tree
FHA	Fault Hazard Analysis
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
FRA	Federal Railroad Administration
FTA	Fault Tree Analysis
HMI	Human Machine Interface
IEEE	Institute of Electrical and Electronics Engineers
MIL-STD	Military Standard
MTTHE	Mean Time to Hazardous Event
MTTR	Mean Times to Repair
O&SHA	Operating & Support Hazard Analysis
PHA	Preliminary Hazard Assessment
PSP	Product Safety Plan
RSPP	Railroad Safety Program Plan
SSHA	Subsystem Hazard Analysis
TWC	Track Warrant Control
TY&E	Train, Yard and Engine Employees
V&V	Verification and Validation

The following definitions of terms are used in this document:

Component	An element, device, or appliance that is part of a system or subsystem.
Hazard	An existing or potential condition that may result in an accident.
Mean Time to Hazardous Event (MTTHE)	The average or expected time that a subsystem or component will operate prior to the occurrence of an unsafe failure.
Previous Condition	Refers to the estimated risk inherent in the portion of the existing method of operation that is relevant to the change under analysis.
Risk	An expression of the possibility/impact of a mishap in terms of hazard severity and hazard probability.
Risk Assessment	The process of determining, either quantitatively or qualitatively, the measure of risk associated with using the processor based signal and train control system or the previous condition.
Safety-critical	A term applied to a function, a system, or any portion thereof, means the correct performance of which is essential to safety of personnel and/or equipment; or the incorrect performance of which may cause a hazardous condition or allow a hazardous condition that was intended to be prevented by the function or system to exist.
Safety Validation	The process of determining whether a product's design requirements fulfill its intended design objectives during its development and life cycle. The goal of the validation process is to determine "whether the correct product was built."
Safety Verification	The process of determining whether the results of a given phase of the development cycle fulfill the validated requirements established at the start of that phase. The goal of the verification process is to determine "whether the product was built correctly."

Subsystem	An element of a system that, in itself may constitute a system.
System	Refers to the processor based signal and train control system and includes all subsystems and components thereof, as the context requires.
System Safety Precedence	The order of precedence in which methods used to eliminate or control identified hazards within a system are implemented.
Product Supplier	This can mean internal BNSF personnel or external third party personnel performing the development of a component or components for a safety-critical processor based signal and train control systems, or safety critical subsystems.

2 Applicable Documents

The following documents were used in the preparation of this RSPP. These documents will be kept in a safety library.

a) General Code of Operating Rules Fifth Edition. In effect April 3, 2005 (including revisions up to July 14, 2005).

b) BNSF Railway Air Brake and Train Handling Rules No. 3. In effect July 13, 2003 (including revisions up to June 24, 2005).

c) BNSF Railway TY&E Safety Supplement No. 1. In effect April 1, 1998 (including revisions up to April 3, 2005).

d) BNSF Railway Mechanical Safety Rules and Policies. In effect October 31, 2004 (including revisions up to July 22, 2005).

e) BNSF Railway Employee Safety Rules. In effect October 31, 2004.

f) BNSF Railway Maintenance of Way Safety Rules. In effect January 31, 1999 (including revisions up to April 3, 2005).

g) BNSF Railway Maintenance of Way Operating Rules. In effect October 31, 2004 (including revisions up to April 3, 2005).

h) BNSF Railway Train Dispatcher's, Operator's and Control Operator' s Manual. In effect July 13, 2003 (including revisions up to April 3, 2005).

i) BNSF Railway System Special Instructions, All Subdivisions No. 10. In effect April 3, 2005 (including revisions up to August 18, 2005).

j) 49 CFR Part 236 Subpart H, "Standards for Development and Use of Processor-Based Signal and Train Control Systems; Final Rule" dated March 7, 2005.

k) MIL-STD-882C, "System Safety Program Requirements" with Notice 1, US DoD, 13 March 1996.

l) IEEE STD 610.12-1990, "IEEE Standard Glossary of Software Engineering Terminology" .

m) IEEE STD 730.1-1998, "IEEE Guide for Software Quality Assurance Planning" , the Institute of Electrical and Electronics Engineers, Inc., 1998.

n) IEEE STD 828-1998, "IEEE Standard for Software Configuration Management" , the Institute of Electrical and Electronics Engineers, Inc., 1998.

o) IEEE STD 830-1998, "IEEE Recommended Practice for Software Requirements Specifications" , the Institute of Electrical and Electronics Engineers, Inc., 1998.

p) IEEE STD 982.1-1988, "IEEE Standard Dictionary of Measures to Produce Reliable Software" , The Institute of Electrical and Electronics Engineers, Inc., 1989.

q) IEEE STD 982.2-1988, "IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software" , The Institute of Electrical and Electronics Engineers, Inc., 1989.

r) IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation" , IEEE Computer Society

s) IEEE STD 1016-1998, "IEEE Recommended Practice for Software Design Descriptions" , IEEE Computer Society, 23 September 1998.

t) IEEE STD 1028-1997, "IEEE Standard for Software Reviews" , IEEE Computer Society, 4 March 1998.

u) IEEE STD 1042-1987, "IEEE Guide to Software Configuration Management" , IEEE Computer Society, 10 September 1987.

v) IEEE STD 1058.1-1998, "IEEE Standard for Software Project Management Plans" , the Institute of Electrical and Electronics Engineers, Inc., 1998.

w) IEEE Std 1074-1997, "IEEE Standard for Developing Software Life Cycle Processes" , The Institute of Electrical and Electronics Engineers, Inc., 1998.

x) IEEE STD 1233, 1998 Edition, "IEEE Guide for Developing System Requirements Specifications" , The Institute of Electrical and Electronics, Inc., 1998.

y) IEEE STD 1483-2000, "IEEE Standard for Verification of Vital Function in Processor Based Systems Used in Rail Transit Control" , IEEE Vehicular Technology Society, 30 March 2000.

3 Applicable Systems

The RSPP applies to all Safety-Critical Processor-Based Signal and Train Control Systems subject to Part 236, Subpart H.

The following is a list of currently known applicable systems:

- The BNSF Railway's Electronic Train Management System (ETMS) installed on the BNSF. The initial testing and deployment was performed on the Springfield Division, Beardstown Subdivision, in the state of Illinois, between Mile Post 116x and Mile Post 119, encompassing approximately 130 miles.
- Note: Subsequent deployments of ETMS may include some or all of the subdivisions on the BNSF and include TWC (Non-ABS, ABS) and CTC control types.

4 General Requirements for Development of Safety-Critical Processor-Based Signal and Train Control Railroad Safety Program Plan (RSPP) [49 CFR Subpart H §236 .905]

The Railroad Safety Program Plan (RSPP) serves as the principle safety document for Safety-Critical Processor-Based Signal and Train Control Systems that may be developed, acquired, or installed by the BNSF. The initial RSPP must be submitted to the FRA, by the BNSF, for approval [49 CFR Subpart H §236.905(a)]. This RSPP establishes the minimum Product Safety Plan (PSP) requirements that will govern the application of design, operating, technical, and management techniques and principles throughout the life cycle of the safety-critical processor-based signal and train control system to reduce hazards and unsafe conditions. The safety-critical processor-based signal and train control system PSP is viewed as a living document that will be updated as circumstances change or new information becomes available. Where possible, the development of a system safety plan will precede the design, implementation, and operation of the safety-critical processor-based signal and train control system. The areas identified in the following subsections shall be addressed.

4.1 Requirements and Concepts [49 CFR Subpart H §236.905(b) (1)]

The RSPP shall address minimum requirements for the development of the safety-critical processor-based signal and train control system.

4.1.1 Methods to Evaluate Behavior [49 CFR, Subpart H, §236.905(b)(1)(i)]

Appropriate hazard identification and evaluation techniques shall be used to evaluate system behavior. The risk associated with potential system behavior hazards shall be analyzed as will the design and/or procedural protections against those risks. The preferred approach to this evaluation is to use hazard analysis techniques that assess

the risk associated with the potential system behavior hazards, and provide for design or procedural protections against those risks. Acceptable hazard evaluation methodologies and techniques, among others, that will be used as a part of this process include the following:

- Preliminary Hazards Analysis (PHA)
- Functional Fault Tree (FFT) or equivalent
- Subsystem Hazard Analysis (SSHA)
- Operating & Support Hazard Analysis (O&SHA)

These hazard identification methodologies and the risk assessment process described in the Section 4.1.2 shall be used to establish safety requirements to eliminate, mitigate, or control potential hazards.

4.1.2 Risk Assessment [49 CFR Subpart H §236.905(b)(1)(ii)]

A documented hazard risk assessment shall be performed that ranks each hazard in terms of severity and probability of occurrence. Once a hazard is identified, an analysis of its potential severity and probability of occurrence shall be performed. The process for this analysis shall be standardized[1]. The following categories of probability and severity (taken from MIL-STD-882C) [Ref D] or an approved equivalent shall be used to perform the hazard risk assessment.

Hazard Severity is defined as a subjective measure of the worst credible mishap resulting from personnel error, environmental conditions, design inadequacies, and/or

[1] While it is possible to develop a quantitative methodology for this type of analysis, the most practical method for railroad application is straightforward deductive reasoning, applied on a collective or organizational basis. A composite of experienced railroad personnel from appropriate line and staff departments can effectively determine the severity of all but the most difficult or unusual hazards.

procedural deficiencies for system, subsystem, or component failure or malfunction, and shall be categorized as follows:

I. (Catastrophic)	Events that result in fatalities and/or multiple severe injuries, loss of one or more major systems, or irreversible severe environmental damage.
II. (Critical)	Events that result a single fatality or severe injury, loss a major system, or reversible environmental damage.
III. (Marginal)	Events that result in minor injury, severe system(s) damage, or mitigable environmental damage.
IV. (Negligible)	Events that result in possible single minor injury, system damage, or minimal environmental damage.

Hazard Probability is defined as the probability that a specific hazard will occur during the planned life cycle of the system element, subsystem, or component. Hazard probability can be described subjectively in potential occurrences per unit of time, events, population, items, or activity, and shall be ranked as follows:

A. (Frequent)	Likely to occur frequently in an individual item; may be continuously experienced in fleet/inventory. P(incident) > 1 in 1 million train miles.
B. (Probable)	Will occur several times in life of an item; will occur frequently in fleet/inventory. 1 million train miles >= P(incident) > 10 million train miles.
C. (Occasional)	Likely to occur sometime in the life of an item; will occur several times in fleet/inventory. 10 million train miles >= P(incident) > 100 million train miles.

D. (Remote) Unlikely but possible to occur in life of an item; unlikely but can be expected to occur in fleet/inventory. 100 million train miles >= P(incident) > 1 billion train miles.

E. (Improbable) Very unlikely; it can be assumed occurrence may not be experienced; unlikely to occur, but possible in fleet. P(incident) <= 1 billion train miles.[2]

Hazard Risk Assessment is the process of combining the hazard severity and hazard probability to determine which identified hazards are acceptable as is, acceptable with proper documentation, acceptable with sufficient mitigation, or unacceptable. A hazard risk assessment performed for BNSF will use the following matrix (Table 5.1). The matrix will be used to establish hazard risk, and set priorities for resolutions that eliminate, minimize, or control the hazards.

SEVERITY → / PROBABILITY ↓	I	II	III	IV
A	UN	UN	UN	AC
B	UN	UN	UN	AC
C	UN	UN	AC/WR	AC
D	UN	AC/WR	AC	AC
E	AC/WR	AC	AC	AC

UN - UNACCEPTABLE

AC/WR - ACCEPTABLE WITH REVIEW BY BNSF MANAGEMENT

AC - ACCEPTABLE WITHOUT REVIEW

Table 5.1 Hazard Risk Resolution Matrix

[2] The E (Improbable) category is not interpreted as zero probability, thus zero risk. The E (Improbable) category includes all items that are judged to have low or extremely low probability of occurrence. There is no zero probability category included in the ranking matrix.

Establishment of *safety requirements* shall result from formalized, predetermined procedures for hazard and risk resolution. ***Hazard Resolution*** is defined as the analysis and subsequent actions taken to reduce, to the lowest level practical, the risk associated with an identified hazard. Safety requirements shall be defined for hazards that present a risk that cannot be accepted because of severity and/or high probability ("unacceptable" risk index in Table 5.1) and thus must be eliminated by design or other explicit control measures. Hazards with risk in the "acceptable with review" category shall be subject to appropriate hazard resolution procedures that eliminate, mitigate, or minimize the hazard risk to the satisfaction of BNSF Railway with the approval of the Vice President of Safety.[3]

4.1.3 System Safety Precedence [49 CFR Subpart H §236.905(b)(1)(iii)]

The Product Supplier shall follow the order of precedence for satisfying the safety-critical processor-based signal and train control system safety requirements and resolving identified hazards per this RSPP as follows:

a) Design for minimum risk. Eliminate hazards through design. Minimize or eliminate the use of human input for safety-critical functions. Minimize or eliminate the use of data from external non-safety-critical systems for safety-critical functions. When human input, or data from external non-safety-critical systems is used for safety-critical functions, design to minimize or eliminate hazards from human input error, or from erroneous, out of sequence, or stale data from non-safety-critical systems. If an identified hazard cannot be eliminated, reduce the associated risk to an acceptable level through design selection and proper implementation using Safety Assurance Concepts to the satisfaction of BNSF Railway with the approval of the Vice President of Safety.

[3] Hazard resolution is not synonymous with hazard elimination. In a railroad environment, there are some hazards that are impossible to eliminate and others that are highly impractical to eliminate. Reduction of risk to the lowest practical level can be accomplished by applying appropriate safety design principles. Examples of these safety design principles are provided in MIL-STD- 882C [ref D].

b) Incorporate safety devices. Reduce the hazard to an acceptable level through the use of fixed, automatic, or other protective safety design features or devices. Provisions shall be made for periodic functional checks and calibration of safety devices where applicable. Fail-safe devices may be provided as protection against hazards that can be caused by other system components.

c) Provide warning devices or labels. Use devices to detect potentially hazardous conditions and to produce adequate warning signals to alert personnel of the hazard. Warning signals and labels and their application shall assure a minimal probability of incorrect personnel reaction to the warning signals and shall be standardized within like types of systems.

d) Develop procedures and training. Procedures and training shall only be used with prior BNSF approval where it is impractical to eliminate hazards through design selection or to adequately reduce associated risk with safety and warning devices. Procedures may include the use of personal protective equipment.

4.1.4 Safety Assessment Process Requirements [49 CFR Subpart H §236.905(b)(1)(iv)]

The safety-critical processor-based signal and train control system will be implemented and managed using a comprehensive safety assurance process that addresses the life cycle of the system. This safety assurance process will be focused on identifying and resolving hazards associated with the system. Evidence that the safety assurance process will meet the requirements as established by BNSF and applicable FRA regulation shall be BNSF review and the acceptance of the safety documents. The Product Supplier shall execute and document this process as part of the PSP where

appropriate. The framework of this safety assurance process focuses on the following elements.

- Identifying potential hazards throughout the system life cycle.
- Understanding impact on safety of the potential hazards by quantifying the risk associated with each hazard.
- Establishing hazard-tracking mechanisms to ensure that resolution measures (i.e., system safety requirements, rules, processes, and procedures) are taken as appropriate to eliminate, minimize, or control unacceptable hazards.
- Performing safety V&V to demonstrate system safety.
- Monitoring testing and system operations to ensure achievement of safety requirements.

4.2 Design for Verification & Validation [49 CFR Subpart H Part 236.905(b)(2)]

The safety-critical processor-based signal and train control system development and implementation process shall include safety V&V. System safety V&V comprises a set of safety activities for a system based on a set of analyses, tests, simulations and calculations that together demonstrate compliance with all applicable safety requirements. Safety verification activities shall demonstrate that the system is built correctly, and include those activities that demonstrate the system has been designed and implemented with the required level of safety from a qualitative and quantitative standpoint, including showing that all unacceptable and undesirable hazards have been mitigated or eliminated.

Safety validation activities shall demonstrate that the correct system is built. Safety validation involves those activities that demonstrate the overall integrated system, and each portion thereof, performs the correct safety functions. These safety validation and verification activities help establish the technical evidence of the safety-critical

processor-based signal and train control system safety. A copy of any non-published standards shall be included with the PSP.

To minimize the extent of safety validation and verification required to satisfy the requirements of this RSPP, safety-critical functions shall be designed to be isolated or partitioned to operate as independent of other non-safety-related functions to the greatest extent possible.

4.2.1 Methodology

The RSPP shall identify the validation and verification methods requirements for the preliminary safety analysis, the initial development process and future incremental changes, including standards to be used in the validation and verification process.

4.2.2 Standards

The safety validation and verification activities shall incorporate requirements and guidance from existing standards for safety validation and verification of hardware and software consistent with 49 CFR Subpart H Part 236, Appendix C – Safety Assurance Criteria and Processes. Applicable standards will be identified in the PSP and adhered to throughout the safety validation and verification process. The safety-critical processor-based signal and train control system PSP shall clearly identify individual standards and requirements that will be used in the design, development, installation, and testing of the product. The standards that are acceptable for verification and validation must be sufficient to support the achievement of the requirements of 49 CFR 236 Subpart H. Non-published standards shall only be used with prior BNSF approval.

4.2.3 Documentation Required to Support Independent Audit of Verification and Validation

All safety V&V activities shall be sufficiently documented to record the specific activities undertaken and their results, and shall provide a credible audit trail for project team review and/or a possible independent, third party confirmation that the safety V&V activities were comprehensive and adhered to best practices. The documentation and results of all V&V activities shall be provided and maintained irregardless of the need for a third party audit. Documentation of V&V activities shall include the following requirements:

- Traceability links between all relevant design and safety program documents. This includes linking of identified hazards to their specific mitigation at each level of requirements, design, operational instructions/warnings, and test documentation.
- Description of the safety V&V methodologies employed.
- Identification of standards, processes, and other reference documentation (e.g., design documents).
- Testing methodology, procedures, and test results.
- Description of the specific safety requirement(s) examined in each V&V activity.
- Discussion of qualitative and/or quantitative conclusions resulting from the V&V activity.
- Cross references to previous hazard analyses, the hazard log, hazard resolution actions, evidence that hazards were resolved (controlled, mitigated or eliminated), and the safety V&V activity that demonstrated compliance with safety requirements.

Third party assessment documentation per Appendix D of 49 CFR 236, Subpart H may require the BNSF to provide an independent evaluation of the utilization of safety design

practices during the development and testing phase. General requirements applied to third party assessments include:

- Preservation of the reviewers' independence and maintaining the Product Suppliers' proprietary rights.
- Access to documentation and attendance where possible at design reviews and "walkthroughs" that are deemed necessary.

The following levels of third party evaluation and functionality may occur if required:

Preliminary Level:

- Evaluation of the processes with acceptable methodology including documentation of any identified safety vulnerabilities that are not mitigated
- Evaluation of the BNSF RSPP and PSP

Functional Level:

- Review of the Preliminary Hazard Analysis (PHA), Fault tree Analysis (FTA), and the Fault Modes Effects Criticality Analysis (FMECA) for correctness, completeness and compliance with the BNSF RSPP.

Implementation Level:

- The third party shall randomly select various safety-critical software modules, of sufficient quantity to provide confidence that the total is in compliance with the RSPP, for audit to verify that RSPP requirements are followed.

Final Report:

- The third party shall evaluate and comment on the installation plan and test procedures
- The third party shall prepare a final report of the assessment that contains the following:
  - An evaluation of the adequacy of the PSP, including the Product Suppliers MTTHE and risk estimates, and the Product Suppliers' confidence interval in the estimates; the safety-critical processor-based signal and train control system vulnerabilities which were not adequately mitigated,

including the method by which BNSF would assure the safety-critical processor-based signal and train control system safety in the event of hardware or software failure, and the method by which BNSF addresses comprehensiveness of the safety-critical processor-based signal and train control system design for the requirements of the operation;

- Identifying each vulnerability and clearly stating the position of the Product Supplier and BNSF relating to the vulnerability;
- Identifying any denied, incomplete, or inadequate documentation;
- Listing each RSPP procedure or process which was not properly followed;
- An evaluation of the software V&V procedures for the safety-critical processor-based signal and train control system safety-critical applications;
- Identifying the methods employed by the Product Supplier in developing safety-critical software

4.3 Human Factors Design Requirements [49 CFR Subpart H §236.905(b) (3)]

The PSP shall identify the process used during the safety-critical processor-based signal and train control system development to identify human factors issues and develop design requirements that address layout design used to minimize the risk of human error, attention loss, and operation fatigue. The PSP shall contain a human factors analysis of human-machine interface (HMI) safety functions performed by humans while the system is in operation.

The PSP will identify human factors issues and document the manner in which the design of the safety-critical processor-based signal and train control system addresses each human factor issue identified. The Product Supplier must consider the general functions identified in Appendix E of the 49 CFR, SUBPART H.

The human factors requirements of the safety-critical processor-based signal and train control system shall be consistent with the BNSF operating practices and with railroad rules and procedures for safe operation. Any proposed use of additional railroad rules and/or procedures for safe operation requires prior BNSF Railway Vice President of Safety approval.

4.4 Configuration Management Control [49 CFR Subpart H §236.905(b)(4)]

Formal methods for configuration control and associated documentation shall accompany design and development of the safety-critical processor-based signal and train control system. This documentation shall clearly identify those control measures that manage system safety functional requirements and hazard resolution actions for the system. Such identification will be provided in documents and databases using a consistent symbol, word or unique character that means "safety-critical."

A configuration management (CM) plan establishes the CM practices to be used on all hardware, software and documentation developed for the safety-critical processor-based signal and train control system BNSF will review and approve the Product Suppliers proposed Configuration Management Program to ensure that it is compatible with BNSF requirements and existing methodology. The configuration management plans shall include the methodologies used to track changes, request changes, and summarize change impact analysis for hardware and software changes of the safety-critical processor-based signal and train control system. These control management methodologies shall be approved by the BNSF and contain at least the minimum criteria to satisfy the requirements as mandated by regulatory statues.

Configuration management is a process to:

- Identify and document the functional and physical characteristics of configuration management items that relate to safety critical processor-based signal and train control systems. These items would include hardware management control plans, software management control plans, and a management control plans for any supporting documentation that is crucial to the operation, maintenance, and troubleshooting of the safety-critical processor-based signal and train control system.

- Audit these configuration items to verify conformance to specifications, standards, and other contract requirements.

- Control changes to configuration items and their related documentation.

- Record and report information needed to manage configuration items effectively, including the status of proposed changes and the implementation status of approved changes.

- Report status of the product or system configuration to the appropriate BNSF personnel as necessary.

4.5 Railroad Safety Program Plan Modifications [49 CFR Subpart H §236.905(d)]

BNSF may find the need to modify their RSPP. Modifications to the finalized and FRA approved RSPP will need to be requested and approved through the Office of the Vice President of Safety on the BNSF. Any RSPP modifications related to safety-critical PSP requirements will require additional approval from the FRA.

5 Product Safety Plan (PSP) Requirements [49 CFR Subpart H §236.907]

The Product Supplier shall prepare, with the assistance of BNSF, a Product Safety Plan (PSP) compliant with this RSPP and with applicable FRA regulations for the equipment included in the safety-critical processor-based signal and train control system The PSP shall describe the safety-critical processor-based signal and train control system in detail, both physically and operationally, and must include acceptable procedures for the implementation, testing, and maintenance. The PSP shall contain the minimum requirements described in the subsections listed below.

The minimum requirements described below include various analyses, test results, and other documentation that support the Product Suppliers' safety program and activities. This documentary evidence may be incorporated in the Product Suppliers PSP in its entirety, or prepared as separate documents and appropriately referenced in the body of the PSP. All documentary evidence supporting the Product Suppliers PSP shall be available for review and audit by the BNSF and the BNSF's designee. The Product Supplier must consider the following subsections as the minimum requirements for the PSP.

5.1 Description of the Safety-Critical Processor-Based Signal and Train Control System [49 CFR Subpart H §236.907(a)(1)]

The safety-critical processor-based signal and train control system PSP shall contain a complete description of the system, including a list of the components and their physical relationship. This description shall include the following minimum requirements:

- General description of the safety-critical processor-based signal and train control system and its role in the overall train control system operation, including interfaces and interactions with existing systems and/or equipment.
- Physical description of the safety-critical processor-based signal and train control system including identification of any subsystems and/or modules that makes up the safety-critical processor-based signal and train control system.
- Descriptions of individual subsystems and/or modules including their function within the safety-critical processor-based signal and train control system.
- Evidence that the safety-critical processor-based signal and train control system as designed, manufactured, tested, and assembled will meet the system safety requirements as established by BNSF and applicable FRA regulation by demonstrating system performance and the acceptance of the safety documents.

5.2 Description of Railroad Operation [49 CFR Subpart H §236.907(a)(2)]

The PSP will describe the type of railroad operation where the safety-critical processor-based signal and train control system may be used. BNSF will include the relevant BNSF physical infrastructure and current and planned operations for the subdivisions in the pilot subdivisions. The PSP will also describe the maximum train volume, train frequency, operating speed, and other physical capacities as applicable, for which the system is designed.

5.3 Operational Concepts Documentation [49 CFR Subpart H §236.907 (a)(3)]

The safety-critical processor-based signal and train control system PSP shall describe the operational concepts, the functionality of the various subsystems and/or modules, and information flows within the System. This description will include the safety-critical processor-based signal and train control system operational concepts as defined for both normal and abnormal operating conditions.

5.4 Safety Requirements Documentation [49 CFR Subpart H §236.907(a)(4)]

The PSP shall identify all requirements necessary for the safe operation of the safety-critical processor-based signal and train control system for its intended application. These safety requirements shall include both original and derived requirements and be established through use of accepted analysis techniques as defined by the BNSF and shall include both hardware and software safety requirements as necessary. Each safety requirement shall be further defined by the specific functions that must be implemented in the specific subsystem or component of the safety-critical processor-based signal and train control system in order to satisfy the given safety requirement.

5.5 System Architecture [49 CFR Subpart H §236.907 (a) (5)]

The PSP shall describe the safety-critical processor-based signal and train control system architecture and how the system architecture satisfies each system safety requirement at the overall system level. The system architecture should cover both software and hardware aspects which identify the protection developed against random hardware faults and systematic errors. These System Safety Concepts shall be identified as part of the overall architecture of the system in order to support safe operation.

5.6 Hazard Log [49 CFR Subpart H §236.907 (a) (6)]

A Hazard Log provides a specific description of the hazards that must be addressed throughout the life cycle of the safety-critical processor-based signal and train control system, as derived from the safety-critical processor-based signal and train control system functionality, operating methods, and the hazard analysis. The PSP shall include a formal Hazard Log and describe the methods used for tracking the identified hazards to ensure that these hazards are resolved in the system design.

Each hazard description shall include a stated threshold level (residual hazard risk index) that, if exceeded, would be unacceptable. In addition, any hazard with a hazard severity ranking of I or II shall be designated as a Safety Critical Item and clearly identified as such in the Hazard Log. Safety critical items will require completion of the defined resolution action prior to system operation. The Hazard Log shall be updated throughout the project as actions are completed to resolve the hazards identified and as any new hazards are identified.

The Hazard Log shall contain the following information for each identified hazard and safety-critical item:

- A unique hazard identification number.
- Description of the hazard.
- References to the safety program or development activity where the hazard was identified and source document traceability supporting the hazard identification.
- Risk ranking of the hazard.
- Proposed resolution for the hazard.
- Assignment of responsibility for the resolution action to a program function/organization.
- Status of the hazard resolution action, including actions taken, date of actions, review and approval of the action, and references to source documents supporting the action.
- Notations of whether the hazard is OPEN (requiring further action) or CLOSED (resolution action(s) complete and approved by BNSF).

5.7 Risk Assessment Requirements [49 CFR Subpart H §236.907 (a) (7)]

The PSP shall include a risk assessment of identified hazards consistent with the risk assessment strategy defined in Section 6.2 of this RSPP and section 236.907 (a) (7),

and Appendix B of the 49 CFR, SUBPART H. The risk assessment shall include system hardware, software, human elements, and their interfaces and shall address both hazard severity and probability of occurrence. Hazards initially identified as having an unacceptable or undesirable risk shall be eliminated by design or mitigated such that the risk is acceptable or can be controlled through the appropriate application of existing operating rules, operating practices and/or procedures. Hazards which are introduced by the safety-critical processor-based signal and train control system initially identified as having an unacceptable or undesirable risk shall not be mitigated by the imposition of new operating rules, operating practices, and/or procedures without prior approval of BNSF. The risk assessment shall clearly identify the risks that require mitigation, the mitigation strategy employed, and justification for the determining the reduced risk level. Alternatively, an abbreviated risk assessment may be developed per Section 6.2 of this RSPP if the system introduces no new hazards and the MTTHE is equal to or greater than that of the system it is replacing.

The safety-critical performance of a safety-critical processor-based signal and train control system pilot territory for which risk assessment is required shall be assessed in accordance with the following criteria.

a) Risk metric expression: The risk metric must describe with a high degree of confidence the accumulated risk over a life cycle of 25 years. The risk metric must be expressed with an upper bound, as estimated with a sensitivity analysis.
b) Interconnected subsystems/components: The safety-critical assessment must include the entire safety-critical processor-based signal and train control system interconnected subsystems and components and their interaction.
c) Computing previous condition: The subsystems or components of the previous condition must be analyzed with a Mean Time to Hazardous Event (MTTHE).
d) Including major risks: The risk calculation must consider the method of operation as subjected to a list of hazards on the pilot territory to be mitigated by the safety-

critical processor-based signal and train control system. The methodology requirements may include the following major characteristics:

1. Track plan infrastructure;
2. Total number of trains and movement density;
3. Train movement operational rules, as enforced by the dispatcher and train crew behaviors;
4. Wayside subsystems and components; and
5. On-board system and components.

e) Other relevant parameters: Failure modes must be determined for the integrated hardware/software as a function of Mean Times to Failure (MTTF), failure restoration rates. Train operating and movement rules along with components that are layered must be considered. System safety-critical design for V&V must support the risk oriented assessment and validate the methodology used to arrive at the assessment results.

f) Assessing the safety-critical processor-based signal and train control system subsystems and components:

1. An MTTHE value must be computed for subsystems and components of the safety-critical processor-based signal and train control system indicating the safety-critical behavior of the integrated hardware/software. The human factor impact must be included in the assessment to provide an integrated value. MTTHE calculations must consider
   a. Transient hardware failure rates
   b. Coverage of the integrated hardware/software (application, executive, input/output driver software)
   c. Subsystem or component phased interval maintenance
   d. Restoration rates in response to detected failures
2. MTTHE compliance V&V must be based on the assessment of the design for the V&V process, historical performance data, analytical methods and experimental safety-critical performance testing. The compliance process

must be demonstrated to be compliant and consistent with the MTTHE metric and demonstrated to be compliant and consistent with the MTTHE metric and demonstrated to have a high degree of confidence.

g) Assessing non-processor-based subsystems/components:

1. The safety-critical behavior of all non-processor-based components of the processor-based signal and train control system must be quantified with an MTTHE metric. The MTTHE assessment methodology must consider the permanent and transient hardware failure rate, phased interval maintenance and fault coverage for each non-processor-based subsystem or component and the restoration rate.
2. MTTHE compliance V&V must be based on the assessment of the design for V&V process, historical performance data, analytical methods and experimental safety-critical performance testing performed on the subsystem or component.

h) Documentation:

1. Any assumptions regarding the reliability or availability of mechanical, electric, or electronic components will be documented. The assumptions will include Mean Times to Failure (MTTF) projections, as well as Mean Times to Repair (MTTR) projections, unless it is identified in the risk assessment as not relevant. Comparison to in-service experience will be required.
2. Any assumptions regarding human performance. The documentation shall be in a form as to facilitate later comparison with in-service experience.
3. Any assumptions regarding software defects. The assumptions shall be in a form that permits projecting the likelihood of detecting an in-service software defect. The documentation shall be in a form as to facilitate later comparison with in-service experience.

4. All of the identified safety-critical fault paths must be documented. The documentation shall be in a form as to facilitate later comparison with in-service experience.

5.8 Hazard Mitigation Analysis [49 CFR Subpart H §236.907 (a) (8)]

The PSP shall employ a hazard mitigation analysis to document the process and techniques employed to investigate the consequences of various hazards. All hazards addressed in the system hardware and software including failure mode, a possible cause if identifiable, effect of failure, and remedial action shall be listed in a hazard log. Hazards associated with the safety-critical processor-based signal and train control system will be identified, with particular focus on hazards found to have significant safety effects. Steps taken to identify, eliminate, mitigate, or control hazards shall be documented.

Refer to the methodologies or techniques (referenced below in sections 5.8.1 through 5.8.4) generally accepted for performing these activities include:

- Preliminary Hazard Analysis (PHA)
- Functional Fault Tree (FFT)
- Subsystem Hazard Analysis (SSHA)
- Mean Time to Hazardous Event (MTTHE) value

5.8.1 Preliminary Hazard Analysis (PHA)

The Preliminary Hazard Analysis (PHA) is used to identify possible hazards associated with the top-level functional requirements for the safety-critical processor-based signal and train control system. The results of the PHA identifies high level safety hazards associated with the system and helps define mitigation measures for these hazards early in the system life cycle. The PHA shall consider the system concept, operating

and support constraints and the specific operating environment where the safety-critical processor-based signal and train control system will be implemented.

Documentation for the PHA shall include definition of the system concept as evaluated, description of the methodology employed, list of hazards identified, and potential mitigation measures for those hazards. The PHA is further documented through the use of a hazard log that lists

- Hazard identification number
- Description of the hazard
- Conditions (e.g., design features, operations, support requirements) that contribute to the hazard
- Consequences or Effects of the hazard
- Resolution measures that eliminate, mitigate, or control the hazard (Resolution to a hazard maybe documented elsewhere in the PSP, if applicable.)
- Risk assessment of the hazard in terms of hazard severity and hazard probability (RSPP, Section 4.1.2).

Sufficient references must be provided with the documentation to permit tracking of the hazard from identification through eventual resolution.

5.8.2 Functional Fault Tree (FFT)

A Functional Fault Tree (FFT) assists in organizing the results of a PHA to establish and trace the link between the safety-critical processor-based signal and train control system and component failures to the hazards resulting from these failures. The documentation must illustrate the interrelationships of the hazards, identifying the combinations of faults that contribute to the safety-critical processor-based signal and train control system hazards. These faults are represented as subsystem functions and interfaces with the safety-critical processor-based signal and train control system.

The development of the FFT begins with identification of a top-level safety-critical processor-based signal and train control system hazard from the PHA (e.g., train-to-train collision). Defining the hazards and/or faults that are necessary to result in the hazard defined on the previous level develops each succeeding level of the FFT. Each hazard is developed to the level of specific subsystem faults and/or interface requirements, described as terminal events. The terminal events receive further analysis during the implementation V&V process that examines the hardware and software implementation of the safety-critical processor-based signal and train control system. Terminal events that were not identified during previous analysis shall be tracked for future resolution.

Documentation for the FFT shall include a description of the methodology employed, explanation of hazards/faults represented by the terminal events, and a diagram showing the development of the FFT and the relationships of the terminal events to the top-level train control system hazard. Sufficient references shall be provided with the documentation to permit tracking of the faults through future analyses and eventual resolution.

Acceptable equivalent methods to the FFT might include the Master Logic Diagram (MLD)[4] or a hierarchical list of potential accidents and faults. The MLD is structurally equivalent to the FFT and identifies high-level faults that contribute to an undesired hazard or accident. A hierarchical list is an experienced-based tool that lists potential accidents for a system and contributing causes to those accidents. The list shall be updated (e.g., with the results of a PHA) with new accidents and/or hazards with the introduction of new technology to remain comprehensive.

Fault trees analyses can be either qualitative or quantitative. Qualitative fault trees are effective means of evaluating cut sets and common cause failures while quantitative

[4] PRA Procedures Guide, NUREG/CR-2300.

trees can estimate the probability of hazard occurrence. The development of any alternate analysis intended to replace a fault tree shall be approved by BNSF prior to commencement.

5.8.3 Subsystem Hazard Analysis (SSHA)

The Subsystem Hazard Analysis (SSHA) is created as the final or detailed analysis of the hazards presented by various failures of the system as designed. The SSHA expands the PHA to provide additional detail to the subsystem and interface level faults that contribute to system hazards, and addresses subsystem failure modes, data quality and data communications, and interfaces with existing train control systems. The SSHA must also consider the various operating modes of the safety-critical processor-based signal and train control system and specific interactions and interfaces with any existing operational and wayside equipment and conditions to examine their effects on the safety-critical processor-based signal and train control system. The SSHA may be conducted in the format of a Failure Modes, Effects and Criticality Analysis (FMECA). The objective of this analysis is to identify various hazards and their associated risks, and to develop the means of eliminating hazards or reducing their risks to acceptable levels. The analysis also provides input to the V&V requirements and provides a measure of thoroughness to the V&V activities.

Documentation for the SSHA shall describe the analysis methodology employed, the failure modes examined, how these failure modes reveal themselves in system operation, determination of failure mode risk (severity and probability rankings, RSPP, Section 5.3), and resolution measures to eliminate, mitigate, or control the identified hazards. Sufficient references must be provided with the documentation to permit tracking of the hazards through future analyses and eventual resolution

5.8.4 Mean Time to Hazardous Event (MTTHE) value

Each subsystem or component of the previous condition must be analyzed with a Mean Time to Hazardous Event (MTTHE). An MTTHE value must be calculated for each

safety-critical processor-based signal and train control system subsystem and component, including the safety-critical behavior of the integrated hardware/software subsystem and/or component.

5.9 Verification and Validation Process and Documentation [49 CFR Subpart H §236.907 (a) (9)]

The PSP shall describe the V&V activities performed during the development and define the V&V process necessary to safely deploy the safety-critical processor-based signal and train control system. The PSP shall describe how the following Appendix C subject areas are addressed directly, addressed using other safety criteria, or are not applicable. Third party V&V assessment requirements, if necessary, for the safety-critical processor-based signal and train control system are identified in Appendix D.

a) Minimum criteria and processes for safety analyses conducted in support of the PSP are documented in Appendix C of 49 CFR Subpart H. The analysis must:
   1. Address each paragraph
      a. Explain how the requirements were satisfied or why they are not relevant
   2. Employ a validation and verification process pursuant to paragraph c.

b) The Product Supplier shall address each of the following safety considerations. In the event that any of the principles are not followed, the PSP shall state both the reason(s) for departure and the alternative(s) utilized to mitigate or eliminate the hazards associated with the design principle not followed.

   1. Normal operation: The system must demonstrate safe operation with no hardware failures under normal operating conditions (all safety-critical functions must be performed properly) with proper inputs and within the expected range of environmental conditions. Operations with the safety-critical processor-based signal and train control system must not depend upon the correctness of actions

or procedures used by operations personnel. There must be no hazards that are categorized as unacceptable or undesirable. Hazards categorized as unacceptable must be eliminated by design.

2. Systematic Failure: The safety-critical processor-based signal and train control system must be shown to be free of unsafe systematic failure (those which can be attributed to human error that could occur at various stages throughout product development). This includes unsafe errors in the software due to human error in software specifications, design and/or coding; human errors that could impact hardware design; unsafe conditions that could occur because of an improperly designed human-machine interface; installation and maintenance errors; and errors associated with making modifications.

3. Random failure:
    a. The safety-critical processor-based signal and train control system must be shown to operate safely under conditions of random hardware failure. Frequency of attempted restarts must be considered in the hazard analysis.
    b. The safety-critical processor-based signal and train control system shall allow no single point failures that can result in hazards categorized as unacceptable or undesirable.
    c. If one non-self-revealing failure combined with a second failure can cause a hazard that is categorized as unacceptable or undesirable, then the second failure must be detected and the safety-critical processor-based signal and train control system must achieve a known safe state before falsely activating any physical appliance.

4. Common Mode failure: The safety-critical processor-based signal and train control system, as defined in 49 CFR Subpart H Appendix C (4), must protect

against unsafe conditions that result from two or more subsystems or components intended to compensate one another to perform the same function all fail by the same mode.

5. External Influences: The safety-critical processor-based signal and train control system must be shown to operate safely when subjected to different external influences, including electrical influences, mechanical influences, and climatic conditions.

6. Modifications: Safety must be ensured following modifications to the hardware and/or software.

7. Software: Software faults must not cause hazards categorized as unacceptable or undesirable.

8. Closed Loop Principle: The safety-critical processor-based signal and train control system design must require positive action to be taken in a prescribed manner to either begin operation or continue operation.

c) Acceptable standards for V&V are:
   1. The standards that are acceptable for verification and/or validation of the safety-critical processor-based signal and train control system must be sufficient to support the achievement of 49 CFR 236 Subpart H.
   2. The U.S. Department of Defense MILSTSD 882C (System Safety Program Plan Requirements; Jan. 19, 1993) is recognized as providing an appropriate risk analysis process for incorporation into V&V standards. MILSTSD 882C is and of itself does not constitute a V&V standard.

3. The following additional standards in 49 CFR 236 Subpart H Appendix C (c.) also provides appropriate risk analysis processes, but by themselves do not constitute V&V standards.
4. Other unpublished standards for verification or validation to support the requirements of 49 CFR 236 Subpart H, or provide an appropriate risk analysis process for incorporation into a V&V standard, are acceptable.

Each V&V activity shall be fully documented throughout the V&V process and available to the BNSF or the BNSF designee for audit of the V&V activities.

5.10 Safety Assurance Concepts [49 CFR Subpart H §236.907 (a) (10)]

The safety-critical processor-based signal and train control system documentation shall include a complete description of the safety assurance concepts used in design, including an explanation of the design principles and assumptions. The PSP shall include the results of the safety assessment process by analysis that identifies each potential hazard and an evaluation of the events leading to the hazard; identification of safety-critical subsystems; the safety integrity level of each safety-critical subsystem; design of each safety-critical subsystem; results of a safety integrity analysis to access the safety integrity level achieved by the safety-critical subsystems; and ensure from the analysis that the safety integrity levels have been achieved. The fundamental design principles and application assumptions for the safety assurance concepts must be identified along with the appropriate verification methods to assure the concepts are correctly implemented in the Product Supplier's design.

The safety concepts must have: a) a fundamental premise; b) specific assumptions as to operating environment; c) certain dependencies on completeness of concept application; and d) specific methods that are used to verify the concept has been adequately applied. The description of the Safety Assurance Concept(s) used in the

safety-critical processor-based signal and train control system shall each be described with regard to the four characteristics a) to d) above.

5.11 Human Factors Analysis [49 CFR Subpart H §236.907 (a) (11)]

The PSP shall include a human factors analysis that identifies human machine interfaces that are important to safe operation and maintenance of the safety-critical processor-based signal and train control system. The analysis shall describe the type of human action or function that is required to ensure safety, describe the designed features of the equipment to facilitate human interaction with the equipment, and provide justification of how these design features reduce the potential for human error during operation and maintenance of the equipment.

The human factors analysis shall include a complete description of all human-machine interfaces, a complete description of all functions performed by humans in connection with the safety-critical processor-based signal and train control system to enhance or preserve safety, and an analysis describing how human factors covered in §236.931 are addressed directly, addresses using other safety criteria, or are not applicable.

The human factors analysis shall demonstrate that the design and implementation of functions are consistent with the BNSF operating practices and with the applicable railroad rules and procedures for safe operation.

The human factors analysis shall list all proposed use of additional railroad rules and/or procedures for safe operation. The acceptance and implementation of any additional railroad rules and/or procedures for safe operation requires approval from the BNSF Railway Vice President of Safety.

The scope and techniques of the human factors analysis shall be adequate to show that the product or system is in compliance with all of the applicable requirements of FRA regulations subpart H, Appendix E or equivalent criteria demonstrated to be equally suitable to the Associate Administrator for Safety.

5.12 Training Requirements [49 CFR Subpart H §236.907 (a) (12)]

The Product Supplier, working with BNSF, shall document in the PSP the training requirements necessary for BNSF personnel to ensure safe operation of the safety-critical processor-based signal and train control system. These training requirements will address installation, normal and abnormal operation, repair, modification, and testing of the system, and will be developed jointly by the Product Supplier and the BNSF. The PSP shall identify the intended audience for each training requirement.

5.13 Test Procedures and Equipment [49 CFR Subpart H §236.907 (a) (13)]

The PSP shall document test procedures and identify requirements for test equipment (as needed) for the maintenance of the safety-critical processor-based signal and train control system equipment to ensure safe operation. The test procedure documentation shall include specific safety test procedures, test equipment requirements, description of acceptable safety test results, and appropriate repair, replacement, and/or modification actions required when test results are deemed unacceptable. The procedures, including any calibration requirements, must be consistent with system needs, and shall contain explanation of any deviation from the recommendations of Product Supplier of the equipment. The following types of testing activity shall be included under this requirement:

- Qualification testing designed to demonstrate that the safety-critical processor-based signal and train control system is suitable for a particular application, performed at the factory, on a test track, or on an operating line of the railroad.

- Installation testing designed to demonstrate that the equipment has been installed correctly.

Test procedures shall address the testing frequency necessary to demonstrate that safety requirements, safety critical hazard mitigation processes, and safety critical tolerances are not compromised over time, through use, or after maintenance is performed.

5.14 Part 236 Rules and Regulations [49 CFR Subpart H §236.907 (a) (14)]

The PSP shall list the rules and regulations of the other subparts (A-G) of Part 236 that do not apply or are satisfied by the safety-critical processor-based signal and train control system using an alternative method, and a complete explanation of the manner in which those requirements are otherwise fulfilled per §§234.275 and 236.901(c). Each citation of a rule or regulation shall be accompanied by a justification of why the rule or regulation does not apply or how the product satisfies the rule or regulation.

5.15 Security of Safety-Critical Systems, Subsystems, & Components [49 CFR Subpart H §236.907(a)(15)]

The PSP shall describe security measures for the protection of the safety-critical processor-based signal and train control system. The security measures shall address train-borne, wayside, and centrally located train control subsystems and/or components as applicable. Security measures shall be designed to limit unauthorized access to and prevent tampering or overriding the safety functions of the system. Specific security measures shall be designed to prevent unauthorized access to and/or spoofing of safety-critical messages wherever these messages are communicated via radio, Internet or public switched network.

5.16 Warnings and Warning Labels [49 CFR Subpart H §236.907 (a) (16)]

The PSP shall include descriptions of all warnings and warning labels that are provided in system manuals or placed on system equipment. These warnings shall address hazards to personnel safety and operations safety when inspecting, testing, or maintaining the safety-critical processor-based signal and train control system equipment.

As noted in the System Safety Precedence called for in Section 4.1.3 of this RSPP, warnings and labels shall be used when other mitigation methods do not eliminate the hazard from affecting system user interfaces. The use of warnings and labels shall not be the primary mitigation for hazards with catastrophic severity. Warnings and labels shall be noted and explained during Product Supplier training for users of the safety-critical processor-based signal and train control system and/or its subsystems.

5.17 Implementation Testing [49 CFR Subpart H §236.907 (a)(17)]

The PSP shall identify specific procedures and test equipment necessary to ensure the safe operation, installation, repair, modification and testing of the product. These procedures must be specific about the methodology to be employed for each test to be performed that is required for installation, repair, or modification including documenting the results of the test.

The PSP shall contain a complete description of all initial implementation testing procedures necessary to establish that safety-functional requirements are met and safety-critical hazards are appropriately mitigated.

The PSP shall contain descriptions of pre-implementation factory testing, field-testing procedures, and cutover testing that will demonstrate that the safety-critical requirements are met and the safety-critical hazards are mitigated to the appropriate

level. Detailed field testing procedures will be used to assure that the safety-critical processor-based signal and train control system is properly installed and documented and identifies measures to provide for the safety of train operations during field test and cutover. Such pre-implementation testing shall be shown (by requirement and/or hazard tracing) to verify the mitigation of all identified hazards by the safety-critical processor-based signal and train control system as developed, the proper use of Safety Assurance Concepts, the implementation of all safety-critical subsystem design requirements, and to validate that the system operates in a safe manner per the overall system requirements and architectural safety concepts.

The Product Supplier shall provide the BNSF with the test plans and procedures developed per this requirement, and obtain approval of test plans and procedures from BNSF, prior to conducting the testing. Post Implementation Validation Testing and Monitoring Procedures [49 CFR Subpart H §236.907 (a)(18)]

The PSP shall identify a complete description of all post implementation testing (validation) and monitoring procedures, including the intervals necessary to establish that safety-functional requirements, safety-critical hazard mitigation processes, and safety critical tolerances are not compromised over time, over use, or after maintenance is performed. In addition, [49 CFR Subpart H §236.907 (a)(18)] section ii requires a complete description of each record necessary to ensure the safety of the system that is associated with periodic maintenance, inspections, test, repairs, replacements, adjustments, and the system' s resulting conditions, including records of component failures resulting in safety-relevant hazards will be provided.

The PSP shall identify a complete description of testing procedures and requirements for maintenance and repair of the components of the safety-critical processor-based signal and train control system. These procedures shall also include how BNSF shall perform the appropriate testing after the disarrangement of these components as a

result of repair or maintenance activities to ensure the component is performing as intended.

The Product Supplier shall provide the BNSF with the test plans and procedures developed per this requirement, and obtain approval by the appropriate official of the railroad, prior to conducting the testing.

5.18 Safety-Critical Assumptions [49 CFR Subpart H §236.907 (a)(19)]

The PSP shall describe the assumptions made in the safety-critical processor-based signal and train control system architecture to ensure that the system meets BNSF requirements for availability without compromising the safety-critical requirements that also apply to the operation. Such descriptions will include, for example, all backup methods for continued safe operation in case of system or sub-system failure. The description of the failure scenario assumptions shall be specific to each unique subsystem or component of the system design.

5.19 Incremental and Predefined Changes [49 CFR Subpart H §236.907(a)(20)]

If applicable, the PSP shall provide a detailed description of any pre-defined changes that may be made after initial implementation and how those changes are included in the other parts of this PSP to preclude having to file an amendment to the PSP. This documentation shall document how these changes satisfy the minimum performance standard (as good as or better than the system it replaces), and do not compromise the system' s safety-critical requirements for hazard mitigation. In addition, this section of the PSP shall define how any changes that involve slightly different specifications are verified and validated for safety-critical functions.

5.20 Communication of Hazards [49 CFR Subpart H §236.907(d)]

The PSP shall specify all contractual arrangements with hardware and software external Product Suppliers for immediate notification of any and all safety critical software upgrades, patches, or revisions for their safety-critical processor-based signal and train control system. Also included in this notification shall be the reasons for such a change and any interim remediation for an identified hazard that can affect the intended purpose of the safety-critical processor-based signal and train control system. These notifications shall be required whether or not the BNSF has experienced a failure of the safety-critical processor-based signal and train control system.

The PSP shall specify the BNSF's procedures for action upon notification of a safety-critical upgrade, patch, or revision for this processor-based system, sub-system, or component, and until the upgrade, patch, or revision has been installed. These procedures shall be consistent with the criterion set forth in § 236.915(d) as if the failure had occurred on that railroad.

The PSP shall identify configuration/revision control measures designed to ensure that safety-functional requirements and safety-critical hazard mitigation processes are not compromised as a result of any such change. The configuration/revision control measures must also include methodologies that allow these changes to be audited.

6 Minimum Performance Standard – Results of PSP for the Safety-Critical Processor-Based Signal and Train Control System [49 CFR Subpart H §236.909]

The safety analysis included in the Product Suppliers PSP will establish, with a high degree of confidence[5] that the implementation of the safety-critical processor-based signal and train control system not result in risk that exceeds the previous condition. BNSF will make sure that the standard is met and will make available to the FRA the necessary analyses and documentation

6.1 Performance Standard for Safety Risk Measurement [49 CFR Subpart H §236.909(a)(b)]

A. The safety analysis must establish with a high degree of confidence that the introduction of the safety-critical processor-based signal and train control system will not result in a risk that exceeds the existing level of operation. A common risk metric shall be used to allow comparison of the safety performance of the existing and the new system under the operating scenario. Faults and failures that must be considered include hardware failures, software errors, human errors, and external influences.

FRA will have access to the necessary BNSF analyses and documentation.

B. 49 CFR Subpart H §236.913 (g) (2) documents the railroads PSP requirements for preparation, and FRA notification.

[5] High degree of confidence means that there exists credible safety analysis that is sufficient to persuade a reasonable decision-maker that the likelihood of the changed condition associated with the new product being less safe than the existing condition is very small (remote).

6.2 Risk Assessment Scope [49 CFR Subpart H §236.909(c)(d)]

The 49 CFR Subpart H [§236.909(c)(d)] identifies the proposed standards for the scope of the risk assessment to be conducted.

1. Abbreviated risk assessment: An abbreviated risk assessment demonstrates that the resulting MTTHE for the safety-critical processor-based signal and train control system is greater than the MTTHE for the existing method of operation. This determination must be supported by a credible safety analysis and concurrence from BNSF that an abbreviated risk assessment is acceptable. Use of AREMA standard development is authorized for abbreviated risk assessment on a case-by-case basis as designated by the BNSF and where appropriate.

   An abbreviated risk assessment may be used in lieu of a full risk assessment to show compliance with the performance standard. The abbreviated risk assessment must show compliance with the performance standard by:

   a) Indicating that no new hazards are introduced as a result of the safety-critical processor-based signal and train control system;
   b) Demonstrating that the severity of each hazard associated with the previous existing method of operation condition does not increase;
   c) Demonstrating that the exposure to such hazards does not change from the previous existing method of operation condition.

2. Full risk assessment: A full risk assessment must address the safety risks affected by the introduction, modification, replacement, or enhancement of a product. This includes risks associated with the previous condition, which are no longer present as a result of the change, new risks not present in the previous condition, and risks neither newly created nor eliminated whose nature (probability of occurrence or

severity) is nonetheless affected by the change. A full risk assessment includes both qualitative and quantitative measures.

a) Safety levels must be measured using competent risk assessment methods and must be expressed as the total residual risk in the system over its expected life cycle after implementation of all mitigating measures. Appendix B – Risk Assessment Criteria provides criteria for acceptable risk assessment methods. Other methods that are accepted standards and practice may be used.
b) The risk level must be adjusted for exposure for the previous condition. Exposure must be expressed as total train miles traveled per year. Severity must identify the total cost, including fatalities, injuries, property damage, and other incidental costs.
c) Planned changes in the physical and operating conditions that are coincident with the introduction of the new processor based product require the adjustment of the previous condition to reflect any associated impact on risk. An example would be the adjustment of the previous system to support higher train speeds.

6.3 Risk Assessment General Principles [49 CFR Subpart H §236.909(e)(2)(3)]

The acceptable methods and the general principles for conducting risk assessments are documented in 49 CFR Subpart H §236.909(e)(2)(3). Three variables must be provided with risk calculations: accident frequency, severity, and exposure. Any concurrent changes in railroad operations such as increased train volumes, passenger volumes, and/or operating speeds resulting from the implementation of the safety-critical processor-based signal and train control system must be analyzed for the total change in risk, and then separately to identify and distinguish risk changes associated with the use of the safety-critical processor-based signal and train control system from risk changes due to changes in operating practices (increased operating speeds, etc.).

7 Implementation and Operation [49 CFR Subpart H §236.915]

Safety-critical processor based signal and train control components, systems, or subsystems may not require FRA approval, but rather an informational filing. Implementation of the safety-critical processor-based signal and train control system shall be in compliance with all requirements with this RSPP and the approved PSP. Evidence of compliance shall be established through review of documentary evidence, safety V&V testing, or other reviews or analyses necessary to establish compliance with safety requirements. Evidence of compliance shall be also documented.

Railroad operations after implementation of the safety-critical processor-based signal and train control system shall remain in compliance with the operational design limits as specified in the PSP. Section 236.915 proposes requirements in addition to those found in the PSP, for the safety-critical processor-based signal and train control system implementation and operation.

7.1 Revenue Service Requirements

The safety-critical processor-based signal and train control system may be placed in service 180 days after submitting an informational filing with the FRA, except as stated in 49 CFR Subpart H §236.913 (a)(2), and (a) (3). Filing date information is referenced in section §236.913 © (2).

Except as stated in §236.913 (a) (3) BNSF may not operate the safety-critical processor-based signal and train control system in revenue service until after the Associate Administrator for Safety has approved the petition for approval.

7.2 Restrictions on Testing of Safety-Critical Processor-Based Signal and Train Control System Components, Systems, or Subsystems

Procedures shall be established to ensure safe train movement and operations during testing of the safety-critical processor-based signal and train control system, modules, systems, or subsystems. These procedures shall be integrated into standard testing and maintenance procedures and training programs for test and maintenance personnel to the satisfaction of BNSF Railway with the approval of the Vice President of Safety.

7.3 System or Subsystem Failures

Failures of the safety-critical processor-based signal and train control system subsystems, or components shall be adjusted, repaired, or replaced without undue delay. The BNSF Railway Vice President of Safety has the responsibility for overseeing, investigating, and taking corrective action in the event of a failure. Causes of failure shall be investigated and where necessary, resolution action taken to prevent or reduce the probability of recurrent failure. Safety of train movements and of roadway workers must be ensured during the adjustment, repair, or replacement process.

8 PSP Review and Approval [49 CFR Subpart H §236.913]

8.1 BNSF Review and Approval of the PSP

Any Product Supplier developed PSP, or Product Supplier/BNSF developed PSP shall be reviewed and approved by BNSF before submission to the FRA. The suitability and readiness for submission of any PSP to the FRA by BNSF shall be the sole discretion of BNSF.

9 System Operations and Maintenance Manual [49 CFR Subpart H §236.919]

An electronic document (in an agreed format) and a combined Operation and Maintenance Manual, herein after referred to as the Manual, shall be delivered to BNSF by the Product Supplier, consisting of all documents specified in the PSP for installation, maintenance, repair, modification, inspection, and testing of the safety-critical processor-based signal and train control system. BNSF will properly catalog the contents of the Manual, and will maintain a copy of the Manual, in the format chosen by BNSF, in all locations where needed to properly perform such tasks. The Manual will be available for inspection by the FRA.

Additionally, current and correct plans and layouts required for the proper maintenance, repair, inspection, and testing of the system shall be delivered by the Product Supplier, and copies, in electronic and/or written form maintained by the BNSF where such products are deployed or maintained. Revision control for both hardware and software shall be included.

BNSF configuration management control will ensure that the current hardware, software, and firmware revisions are identified and included in the Manual and plans where relevant. During the Product Supplier's involvement, the Product Supplier shall also maintain proper configuration control per the approved PSP.

BNSF requires that all safety-critical components be positively identified, handled, replaced, and repaired per specific procedures described by the Product Supplier in the Manual. Such procedures are intended to preserve the safety characteristics of the product and components and shall be specified in the PSP.

The Operations and Maintenance Manual shall be based on the system-specific procedures specified in the PSP and consistent with BNSF overall operating rules and practices. The Manual shall address the following activities associated with the product:

- Installation and Deployment.
- Periodic maintenance and testing.
- Modification.
- Repair.
- Operation under normal and fallback modes.

10 Training and Qualification Program [49 CFR Subpart H §236.921, §236.923, §236.925, §236.927, & §236.929]

BNSF will establish and implement training and qualification programs that provide knowledge and skills required for basic job performance for BNSF workers whose duties require interaction with the safety-critical processor-based signal and train control system. BNSF will retain records showing which BNSF employees are designated as qualified.

Section §236.921 works in conjunction with §236.907, which requires the PSP to provide a description of the training necessary to insure safe installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the safety-critical processor-based signal and train control system. These programs will address the minimum BNSF training and qualification requirements for its workers whose duties include:

- Installing, inspecting, testing, maintaining, modifying, or repairing the safety-critical processor-based signal and train control system, subsystems, or components, including, wayside, or onboard equipment.
- Train dispatching operations within the safety-critical processor-based signal and train control system-territory.
- Operating trains or serving as a train crew member in the safety-critical processor-based signal and train control system territory.
- Roadway workers whose duties require knowledge and understanding of the safety-critical processor-based signal and train control system.

BNSF training programs will address both initial training and continuing training programs necessary to maintain worker skills. Training program design, execution, and

record keeping shall be in accordance with the requirements specified in the related FRA regulations [49 CFR Subpart H §236.921, §236.923, §236.925, §236.927, and §236.929].

11 Human-Machine Interface [49 CFR Subpart H Part 236, Appendix E]

The safety-critical processor-based signal and train control system involves human interaction with potentially complex functions that provide safety to the railroad. BNSF requires that the Product Supplier use ergonomic design criteria as specified in the development of the Human Machine Interface (HMI). The Product Supplier shall describe the proposed HMI features of the system for BNSF approval as part of the design documentation. Proper reference to the specific design documents shall be included in the PSP for completeness.

Proper design of HMI will support vigilant attention by the operating personnel and encourage appropriate action where needed to assure safety of the railroad operation. HMI designers must be familiar with the safety-critical processor-based signal and train control system and its operating environment.

The Product Supplier shall perform design trade-off tests using typical personnel or cite existing BNSF standards to demonstrate to the satisfaction of BNSF that the effectiveness of the HMI has been optimized for the purposes of the system. The Product Supplier approach to the items a-j above shall be documented in the PSP.

The Product Supplier is provided further guidance by reviewing FRA regulations 49 CFR Subpart H Part 236, Appendix E.